17-303-cv

IN THE

United States Court of Appeals

FOR THE SECOND CIRCUIT

HADIT SANTANA,

Plaintiff,

and

VANESSA VIGIL and RICARDO VIGIL,

Plaintiffs-Appellants,

v.

TAKE-TWO INTERACTIVE SOFTWARE, INC.,

Defendant-Appellee.

*On Appeal from the United States District Court
For the Southern District of New York (New York City)*

**DEFENDANT-APPELLEE TAKE-TWO
INTERACTIVE SOFTWARE, INC.'S
ANSWERING BRIEF**

IRELL & MANELLA LLP
Robert M. Schwartz (rschwartz@irell.com)
Victor Jih (vjih@irell.com)
Nathaniel Lipanovich (nlipanovich@irell.com)
Molly Russell (mrussell@irell.com)
Derek R. Flores (dflores@irell.com)
1800 Avenue of the Stars, Suite 900
Los Angeles, CA 90067
(310) 277-1010
*Attorneys for Defendant-Appellee
Take-Two Interactive Software, Inc.*

CORPORATE DISCLOSURE STATEMENT

Defendant-Appellee Take-Two Interactive, Inc. has no parent company.

BlackRock, Inc., a publically held corporation, may own 10% or more of Take-

Two's stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Page

Page

Page

Other Authorities

INTRODUCTION

Plaintiffs-Appellants Richard and Vanessa Vigil ask this Court to reverse the dismissal of their lawsuit at the pleading stage for lack of standing. The district court gave the Vigils three opportunities to explain how they were injured by their complaint's alleged procedural violations of the Illinois Biometric Information Privacy Act ("BIPA"). They failed each time. This Court should recognize the same failings and affirm the district court's decision.

The Vigils' case is part of a trend of "gotcha" lawsuits hoping to monetize harmless—and, at most, procedural—violations of a privacy statute. Even though none of plaintiffs' personal information was ever compromised, no home address, credit card, or driver's license numbers were made public, and no one was even embarrassed, the Vigils seek hundreds of millions of dollars in class compensation to redress the defendant's misdeed of creating a video game that allows the Vigils to insert a player into the game that looks like them. Because they could not articulate a concrete injury from these non-events, their case had no basis to move past the pleading stage. Nothing in their appeal brief favors a different outcome.

Their lawsuit is based on the "MyPlayer" feature of Defendant-Appellee Take-Two Interactive Software's NBA 2K15 and 2K16 basketball video games. That feature allows a user to create a personalized cartoon-like avatar to play basketball against others. It does so by capturing images of the user's face. To

- 1 -

make that sound menacing, the Vigils describe the process as "biometric scanning."

The Vigils' complaint admits that they knew in advance that their faces would be "scanned" and converted into a game avatar, and that the avatar would be visible to others. *See* A.23 ¶¶ 28, 41.[1] It also admits that the Vigils wanted to use the feature anyway, that they each sat for 15 minutes as their faces were scanned, that they created their own avatars, and that they used their avatars to play the game with others. *Id.* ¶¶ 29, 45. In short, the Vigils admit that they knowingly and voluntarily chose to play a game that worked exactly as they expected it to work.

Despite this, the Vigils claim that the MyPlayer feature violates BIPA in five procedural and hyper-technical ways:

1.   They claim that their compliance with the game's on screen notice and assent procedure, in which they saw a warning stating that the feature would take and use their scans and that required them to press "Continue" to proceed, is not a sufficient "writing" to authorize the scanning of their faces.

2.   They claim that their knowing and voluntary act of creating the avatar, and then using it to play against others, is not sufficient "consent" to allow the "disclosure" of their avatar to those players.

---

[1] Citations to "A." refer to pages from the Appendix submitted by the Vigils at Docket Nos. 37-38.

3.   They claim that, even though players are told that the facial scans will be used to create the avatars, Take-Two failed to disclose the specific purpose and length of time for which the scans would be used.

4.   They claim that Take-Two failed to make available a formal retention schedule and destruction guidelines.

5.   Even though no data breach or misuse occurred, they claim that Take-Two should have taken unspecified, but even greater, care to protect their data.

The Vigils concede that this case is based on nothing more than "bare statutory violations" that have not otherwise caused them any harm. *See* Appellants' Br. at 21. They do not claim that their faces were scanned against their will or without their knowledge. They do not claim there was a data breach or that one is likely. They do not allege their biometrics were compromised or shared with any unauthorized person. And they do not allege any misuse of their biometrics. The Vigils do not contend that their face scans have been used for any purpose other than for playing the game, something for which they gave consent.

The district court correctly held that such "bare statutory violations" were insufficient to satisfy Article III's standing requirements. The Vigils do not dispute that, to satisfy Article III, a plaintiff must identify a concrete injury-in-fact. That is measured against the purpose for which the given statute was adopted. The Illinois legislature adopted BIPA's collection, dissemination, and disclosure

requirements to help prevent the compromise of biometric data. Here, no data has been compromised, nor is there an imminent risk of that occurring. The Vigils thus lack any concrete injury and therefore lack Article III standing.

Without concrete harm, the Vigils also cannot establish they have a ***statutory*** right to sue. BIPA grants a right of action to only an "aggrieved" plaintiff—i.e., someone who suffered a real injury. The Illinois legislature has expressly adopted that definition of "aggrieved" in other contexts, and the courts have concurred.

The district court correctly dismissed the complaint with prejudice based on both the lack of constitutional and statutory standing. This Court has the well-established authority to affirm that dismissal on either or both grounds, and should.

STATEMENT OF ISSUES PRESENTED

1.   Did the district court correctly determine that the Vigils lacked standing under Article III based on bare statutory violations of BIPA?

2.   Did the district court correctly determine that the Vigils are not "person[s] aggrieved" entitled to pursue a cause of action under BIPA?

3.   Did the district court have the power to reach the issue of statutory standing and, finding none, to dismiss the complaint with prejudice?

STANDARD OF REVIEW

This Court reviews de novo the dismissal of a complaint pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). *See Toran v. City of Binghamton*,

- 4 -

456 F. App'x 44, 45 (2d Cir. 2012); *Cortlandt St. Recovery Corp. v. Hellas Telecomms., S.à.r.l.*, 790 F.3d 411, 417 (2d Cir. 2015).

STATEMENT OF FACTS

This lawsuit involves NBA 2K15 and NBA 2K16, two basketball-themed video games that Take-Two developed and published. The games include the "MyPlayer" feature, which permits users to create a personalized basketball avatar. A.15 ¶ 1; A.23 ¶ 27. A user can create an avatar by manually varying the size and position of the avatar's nose, ears, eyes, forehead, eyebrows, mouth, facial hair, and other attributes. The user can also control characteristics like eye, skin, and hair color. To create an even more customized avatar, a user can scan his or her face (or someone else's face, or an object, or almost anything else) using a camera attached to the video game console. *See* A.23 ¶¶ 27, 29. After the scanning process is complete, but before the avatar is finalized, the user is prompted to make adjustments to the results of the face scan, so as to change the avatar's face geometry. The user can change the eye position, vary the nose size, or chisel its cheekbones. Thus the finished product may be substantially altered before it is seen by anyone else.

To create a MyPlayer avatar, a user must first pass through a notice screen and agree to the following terms and conditions: "Your face scan will be visible to you and others you play with and may be recorded or screen captured during

gameplay. By proceeding you agree and consent to such uses and other uses

pursuant to the End User License Agreement. www.take2games.com/eula." *Id.*

¶ 28. Only after viewing this screen and pressing "continue" can a user access the

MyPlayer feature. *Id.* A user can then create an avatar by getting close to the

camera and turning his or her head (or anything else) to the left and to the right, as

instructed. A.23-24 ¶ 29. The Vigils estimate that this process takes 15 minutes.

See id. The resulting avatar can then be used for game play.

There is no requirement that the avatar resulting from the MyPlayer feature

actually resemble the user.[2] A user's avatar can vary significantly each time the

user creates one, just as a person's likeness can vary from photo to photo. In fact,

the MyPlayer feature will superimpose on the avatar's "face" any image the user

supplies—such as a friend's face, the head of a pet dog or cat, vegetables, or even

space aliens from Star Wars:

---

[2] The Vigils did not attach their avatars to the complaint. Perhaps that is because
they don't resemble either of the plaintiffs. The district court picked up on that
omission and noted that "The Second Amended Complaint contains no allegations
regarding the quality of the plaintiffs' personalized basketball avatars, such as the
degree to which the digitized faces of the plaintiffs' avatars resembled the
plaintiffs." Dkt. 40, Special Appendix ("SPA.") at 11. Without the Vigils'
account information, Take-Two cannot attempt to find the avatars and show them
to the Court.
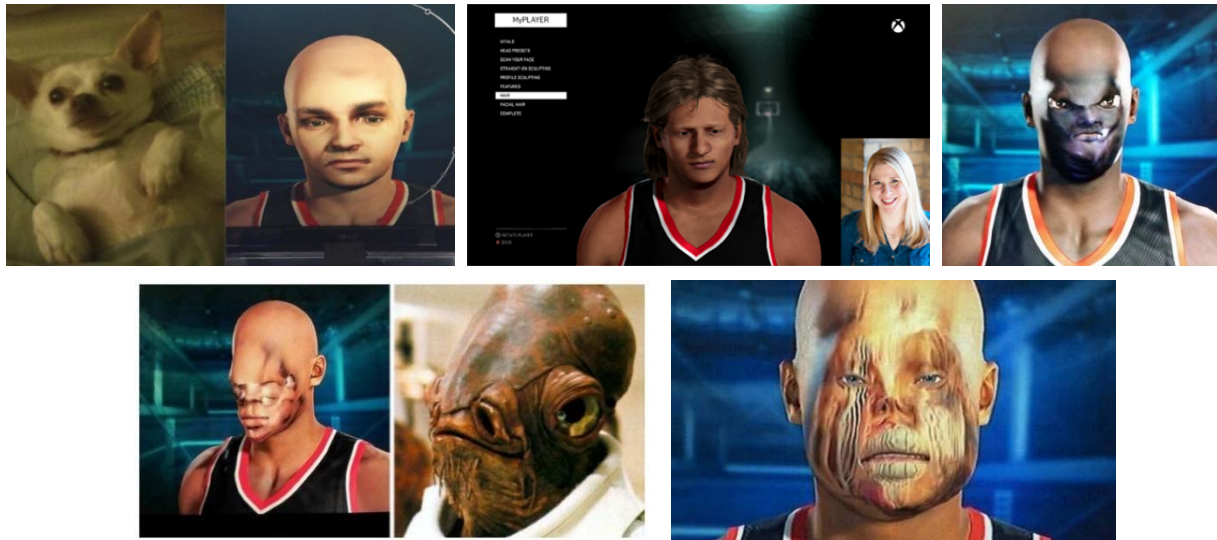
See A.50 (Take-Two's motion to dismiss).

Further, there is no requirement that the person creating the avatar be the person who bought or owns the game, or be the registered account holder. *See, e.g.*, A.26 ¶ 40 (Vanessa Vigil played NBA 2K15 on her brother's account). Thus, an avatar cannot be verifiably linked to any person or account, and the output of the feature is not personally identifying. *See id.* ¶¶ 39-42, A.27 ¶¶ 43-44.

If a user chooses to play with the avatar in "multiplayer" mode, then other players who participate in the same multiplayer game will see the user's avatar during gameplay. *See* A.24 ¶ 31. Take-Two does not make any other use of the avatar data. As the district court explained, "[t]he MyPlayer feature's only alleged purpose is to create personalized basketball avatars." SPA.10 (citing A.23 ¶ 27).

The Vigils allege that they played NBA 2K15 on Mr. Vigil's PlayStation 4. A.26 ¶¶ 39-40. Mr. Vigil alleges that he purchased NBA 2K15, and that the MyPlayer feature was "a material factor motivating [his] decision to purchase the

- 7 -

NBA 2K15 video game." A.28 ¶ 53. Mr. Vigil alleges that he used the MyPlayer feature to scan his face and create an avatar, and that he used it in a multiplayer game. A.26 ¶ 39, 41; A.27 ¶ 45. His sister, Vanessa Vigil, says that she used his copy of the game and that she scanned her face to create an avatar on his console. A.26 ¶¶ 40-42.

The Vigils admit that they consented to the recording and disclosure of their "face scan" before using the MyPlayer feature. *Id.* ¶ 41 ("[E]ach Plaintiff pressed 'Continue' when presented with the screen stating that '[y]our face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay.'"). After pressing "Continue," the Vigils "look[ed] directly into the PlayStation Camera, at which point the PlayStation Camera and the game scanned and analyzed each Plaintiff's face." A.26-27 ¶ 42. The scanning process required the Vigils "to get very close (6-12 inches) to the camera and slowly turn their heads 30 degrees to the left and to the right during the scanning process," which "takes about 15 minutes." A.23-24 ¶ 29.

At oral argument, the Vigils confirmed that they knew their facial scan was being taken during this process, and that it was going to be used to create an avatar for multiplayer game play. A.359:12-17.

The Vigils allege that they then entered a multiplayer game, and that, as a result, the avatar (i.e., the "facial rendition" the Vigils claim is biometric

- 8 -

information under BIPA) "was disclosed and disseminated to other players." A.27

¶ 45. To be accurate, their *avatars* were visible to others. But the underlying

"scan" data, from which their avatars were created, was not. Their claim is even

more watered down. The Vigils' counsel conceded during oral argument that the

Vigils were *not* basing their BIPA claims on the disclosure of their avatars during

multiplayer game play, *see* A.359:12-17, and there is no allegation that the Vigils

biometric data was "disseminated in any form *other than to the gamers who played*

in multiplayer games with the plaintiffs." SPA.13 (emphasis added).

The Vigils do not contend that their identities were stolen, or that their

biometrics have been improperly shared with any third party or otherwise misused,

breached, or compromised. SPA.27. Counsel for the Vigils confirmed this:

> THE COURT: Okay. So, the actual harm is the fact that the image
> was taken and stored in violation of the statute?
>
> PLAINTIFFS' COUNSEL: Correct.
>
>   *   *   *
>
> THE COURT: You're not contending that they misused the
> information, sold the information, gave it to third parties, right?
> That's not part of the complaint. That's not part of your allegation of
> actual harm. Your actual harm is your client had the client's face
> scanned, and they stored it. Right?
>
> PLAINTIFFS' COUNSEL: That they have it, correct. That they
> possess it without my clients' consent.

A.85:18-21, 88:3-10. As the district court summarized, the Vigils "do not contend that their face scans have been disseminated, or used for any purpose, other than for playing the video game, for which they gave consent." SPA.2.

The Vigils nonetheless argue that Take-Two violated BIPA in five ways: (1) Take-Two collected their biometrics without the written authorization and release required by Sections 14/15(b)(1) and (b)(3); (2) Take-Two disseminated their biometric information without the consent required by Section 14/15(d); (3) Take-Two failed to inform the Vigils about the "specific purpose and length of time" for which the biometric data would be stored in violation of Section 14/15(b)(2); (4) Take-Two failed to adopt and make available a formal retention schedule and guidelines for permanently destroying biometrics in violation of Section 14/15(a); and (5) Take-Two failed to handle their biometrics with sufficient care in violation of Section 14/15(e). Appellants' Br. at 29-30. Take-Two disputes these allegations but, for purposes of testing plaintiffs' standing, does not contest them.

SUMMARY OF TAKE-TWO'S ARGUMENT

Under *Spokeo* and *Strubel*, the Vigils bear the burden of showing that the alleged BIPA violations resulted in a concrete injury sufficient to confer Article III standing. The Vigils set forth five "bare statutory violations" as the basis for their alleged standing, and no other injury. Thus, evaluating their right to proceed

requires the Court to determine the concrete interest underlying BIPA and the

relationship between that interest and the alleged statutory violations.

The Illinois Legislature enacted BIPA to secure its residents' biometrics

from compromise and identity theft. To provide these protections, BIPA creates

disclosure, consent, and retention requirements for private entities that obtain

and/or disseminate biometric information. Relying on BIPA's text, and the

legislative findings set forth within BIPA, the district court correctly determined

that BIPA's specific concrete interest is biometric data protection.

On appeal, the Vigils argue that BIPA's concrete interest is much wider, and

consists of an interest in "biometric privacy" in general. However, the Vigils'

argument is based on their own *ipse dixit* and little else. They point to the word

"Privacy" in BIPA's title, but the word "Privacy" begs the question of whether the

Illinois legislature was concerned about a consumer's interest in the ***protection*** of

biometric data (which obviously affects one's privacy interests) or something

much broader. Under Illinois rules of statutory construction, the title does not

control over the text of the statute. Thus this Court should confirm the district

court's holding that BIPA's concrete interest is the biometric data protection

interest set forth in the explicit legislative findings at the beginning of the statute

and not the broad, abstract, and undefined interest in "privacy" the Vigils advocate.

Indeed, the Vigils' shift to a more generalized interest in privacy is a losing

- 11 -

strategy: The more generalized an interest is, the less concrete it is for purposes of satisfying Article III.

The alleged violations in this case do not present any harm or imminent risk of harm. The Vigils complain that Take-Two uses an on screen "pop-up" message that alerts users that they are about to allow the game to capture their images and tells them the uses to which the scans will be put, and then requires users to press "Continue" before the scanning can begin. The Vigils claim that the statute requires a more formalistic version of "written" authorization. The Vigils object to the fact that Take-Two used the words "face scan" instead of "biometric identifier." They complain that Take-Two did not make available a retention schedule and destruction guidelines. None of these issues creates any harm beyond the statutory violations themselves. The Vigils thus lack standing under Article III.

Even if the Vigils' allegations could satisfy Article III, BIPA requires more than a bare statutory violation before a plaintiff can sue. BIPA limits its cause of action to a "person aggrieved." Courts have consistently held that a person must be injured—beyond a statutory violation—to meet that requirement. The Vigils' contrary interpretation of "aggrieved" would read that term out of the statute. Thus, the lack of harm means the Vigils also lack statutory standing.

Finally, the Vigils assert that a court should not have dismissed the case with prejudice, given its ruling that they lack Article III standing. While it is generally

correct that courts without jurisdiction cannot decide merits issues, the Supreme

Court has held that statutory standing is an exception to that rule and can be

decided even in the absence of Article III standing. Here, the district court

properly dismissed with prejudice after deciding the threshold question of whether

the Vigils could sue as "aggrieved" persons under BIPA. A court's discretion to

decide such threshold issues despite Article III concerns is well-established under

Supreme Court and Second Circuit precedents. This Court has the discretion to

affirm the district court's dismissal on either or both grounds.

LEGAL DISCUSSION

I.   THE VIGILS FAIL TO ALLEGE A CONCRETE INJURY AND THUS LACK ARTICLE III STANDING.

A.   Under *Spokeo* And *Strubel*, Plaintiffs Must Establish A Concrete Injury Tied To BIPA's Core Legislative Purpose.

As the party seeking to invoke federal jurisdiction, to establish Article III

standing, a plaintiff has the burden of establishing an injury in fact that is "concrete

and particularized" and "actual or imminent, not conjectural or hypothetical."

Strubel v. Comenity Bank, 842 F.3d 181, 187-88 (2d Cir. 2016). At the pleading

stage, a plaintiff "must clearly allege facts demonstrating" that injury. *Spokeo, Inc.*

v. Robins, 136 S. Ct. 1540, 1547 (2016). Those allegations must be plausible; a

court is not required to draw all inferences in a plaintiff's favor. *See J.S. ex rel.*

N.S. v. Attica Cent. Schs., 386 F.3d 107, 110 (2d Cir. 2004).

On appeal, the Vigils argue that "bare statutory violations" of BIPA, that is, violations without any harm beyond the violations themselves, suffice to confer Article III standing. Appellants' Br. at 5-6, 21.[3] In *Spokeo*, however, the Supreme Court refused to confer standing on one who alleged simply a statutory violation: "Article III standing requires a concrete injury, even in the context of a statutory violation." *Spokeo*, 136 S. Ct. at 1549. Although "Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law,'" a plaintiff will not be able to satisfy the demands of Article III by alleging a "bare [statutory] violation" where it "may result in no harm" or not "present any material risk of harm." *Id.* at 1549-50.

In *Strubel*, this Court clarified how *Spokeo* applies to a bare statutory violation. A court's first step is to determine the concrete interest that the given statute was enacted to protect. *Strubel*, 842 F.3d at 190; *Spokeo*, 136 S. Ct. at

---

[3] When the district court gave the Vigils an opportunity to amend their complaint to allege harm in light of *Spokeo*, they "also alleged that Take-Two unjustly enriched itself by profiting from the realism that gamers' biometric data provided to the gaming experience and, in the case of Ricardo Vigil, that Take-Two caused him actual monetary damages in the amount of the purchase price of the NBA2K15 video game." Appellants' Br. at 19 n.6. Take-Two explained why these theories of harm failed in its renewed motion to dismiss, A.53-59, and the district court agreed they were without merit. SPA.36-45. On appeal, the Vigils do not address these additional theories (other than note them in a footnote) and have limited their argument to the "bare statutory violations" of BIPA. As such, they have waived these theories of harm. *See LoSacco v. City of Middletown*, 71 F.3d 88, 92 (2d Cir. 1995) (waiver of issues by failing to brief them on appeal).

1549. The next step is to determine the relationship between that express concrete interest and the alleged statutory violation.

There can be two outcomes. On the one hand, the relationship can be substantive in nature, where the statute "directly forbids" the **harm** that the statute seeks to prevent. There, before conferring standing, the court examines violations of substantive provisions to confirm that they are sufficiently definite and tied to that harm. *See, e.g.*, *Aranda v. Caribbean Cruise Line, Inc.*, 202 F. Supp. 3d 850, 857 (N.D. Ill. 2016). On the other hand, the relationship can be viewed as merely procedural, where the statute "require[s] the adoption of procedures to decrease congressionally-identified risks." Before conferring standing, the court examines violations of such procedural provisions to confirm that there is an actual injury, or material risk of injury, to the concrete interest behind the statute. *Id.*; *see Strubel*, 842 F.3d at 188-89. The court correctly applied this *Spokeo/Strubel* framework.

B. The District Court Correctly Determined That The Concrete Interest Protected By BIPA Is Biometric Data Protection.

BIPA is a 2008 Illinois statute that addresses biometrics "used to access finances or other sensitive information." 740 Ill. Comp. Stat. 14/5(c) (2008). Noting that the "use of biometrics is growing in the business and security screening sectors," the Illinois legislature sought to safeguard "financial transactions, including finger-scan technologies at grocery stories, gas stations, and school cafeterias." *Id.* at 14/5(a), (b), (c). Biometrics "are biologically unique to the

individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.* at 14/5(c). To prevent this "compromise" of biometrics, BIPA provides disclosure, consent, and retention requirements for private entities that obtain and/or disseminate biometric information. *See* SPA.6; 740 Ill. Comp. Stat. 14/15.

Based on these legislative findings, set forth in the text of BIPA, the district court concluded that the concrete interest protected by BIPA is biometric data ***protection***: "the purpose of the BIPA is to ensure that, when an individual engages in a biometric-facilitated transaction, the private entity protects the individual's biometric data, and does not use that data for an improper purpose, especially a purpose not contemplated by the underlying transaction." SPA.6.

On appeal, the Vigils argue that the purpose of BIPA is not limited to biometric data protection but is rather a generalized (and undefined) interest in "privacy." *See* Appellants' Br. at 24 ("concrete interest in keeping his or her personal biometric data private" and referencing "a general right to privacy"); *id.* at 27 ("biometric privacy as the interest underlying BIPA").

But in determining the concrete interest, the "proper place to begin the analysis of a statute is its text"—not what one imagines could be or what an advocate argues should be the animating interest. *Entergy Nuclear Vt. Yankee,*

LLC v. Schumlin, 733 F.3d 393, 414 (2d Cir. 2013); *see also Disabled in Action of*

Metro. N.Y. v. Hammons, 202 F.3d 110, 124 (2d Cir. 2000).

As the district court noted, there is nothing in the text that reveals any stated

intent to redefine or expand "privacy" substantively, to make the voluntary

disclosure of biometrics more difficult, or to discourage the use of biometrics.

SPA.6, 40. Rather, the legislative findings are specific and express a concern

about biometric information being "compromised," the "heightened risk for

identity theft," and the public's willingness to engage in biometric identifier-

facilitated transactions as a result of that risk. 740 Ill. Comp. Stat. 14/5(c), (e).

Not every provision in a statute *is* the core interest of that statute. A

provision can serve the core interest, but its mere presence is not sufficient to

establish that it is the core interest. On its face, BIPA's core interest is to prevent

the improper disclosure of biometric data. The five provisions the Vigils invoke

serve that interest; they do no more than decrease the risk of that happening and are

therefore merely procedural. *Aranda*, 202 F. Supp. 3d at 857.

The Vigils attempt to support their effort to broaden BIPA's concrete

interest by pointing to its title, which includes the word "Privacy." Appellants' Br.

at 26. But the appearance of the word "Privacy" in the title only begs the question:

"Yes, the statute concerns privacy, but what privacy-related matters does it

concern?" No one disputes data protection and preventing identity theft "concern"

- 17 -

privacy. The single word "Privacy" does not, by itself, signal whether the concrete interest underlying BIPA is the specific—and narrower—interest in actually protecting the information (as the legislative findings suggest) or a much broader one (as Appellants prefer).[4]

Illinois courts have cautioned against the folly of discerning legislative intent from the title of a statute. *See, e.g.*, *Illinois Bell Tel. Co. v. Illinois Commerce Comm'n*, 840 N.E.2d 704, 713 (Ill. App. Ct. 2005) ("As a rule[,] the words of the heading[,] being more general[,] will not control the more specific words of the act"); *Michigan Ave. Nat'l. Bank v. Cty. of Cook*, 714 N.E.2d 1010, 1016-17 (Ill. App. Ct. 1999), *aff'd*, 732 N.E.2d 528 (Ill. 2000) ("The official heading or title of a statute can only provide guidance in interpreting an ambiguous provision.").

This Court's decision in *Strubel* illustrates how focusing on a single word in the title could lead to an erroneous decision. There, the plaintiff alleged that the defendant violated the Truth in Lending Act ("TILA"), in part, by failing to clearly

---

[4] The Vigils also note that BIPA regulates the collection of biometric information. Appellants' Br. at 25-26. As the district court concluded, however, these collection regulations are procedural rules designed to minimize the risk that biometric data will be compromised—the core interest of BIPA. SPA.28-35. Despite what Appellants suggest, the words "collect[ed] without authorization" do not appear in the legislative findings as the intent of BIPA. Appellants' Br. at 27. A reference to "collection" does appear in subsection (g), which makes clear that "regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information" is merely the method by which BIPA's interest is to be safeguarded. 740 Ill. Comp. Stat. 14/5(g).

advise her of its obligation to report within 30 days whether a reported billing error

had been corrected. 842 F.3d at 192. Citing TILA's "declaration of purpose"

provision, this Court identified the statute's "core object" as "avoid[ing] the

uninformed use of credit." *Id.* (quoting 15 U.S.C. § 1601(a)). Assuming that the

defendant lender violated its notice obligations, this Court explained that such a

violation still did "not create the material risk of harm" to a borrower's "interest in

avoiding the uninformed use of credit" "necessary to demonstrate concrete injury."

That is because a failure to disclose what the lender's obligations are does not

directly impact how a borrower might use their credit. *Id.* at 192-93.

Had the Court defined TILA's interest based on the word "Truth" in the title

of the statute, the failure to disclose would have directly impacted a more

generalized interest in "truth." But such an approach would not only mean that this

Court should have decided *Strubel* in the opposite way, it is would be easy to

manipulate, and it ignores the specific indications of intent Congress articulated,

which focus on how a borrower "uses" credit.

The two cases the Vigils cite do not support their assertion that the core

interest behind BIPA is a generalized concern over "privacy." *See* Appellants' Br.

at 27-29. Neither *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d

1155 (N.D. Cal. 2016), nor *Rivera v. Google Inc.*, 2017 WL 748590 (N.D. Ill. Feb.

27, 2017), addressed what BIPA's core interest is.

In *Facebook*, the defendant invoked the California choice-of-law provision in Facebook's Terms of Use as grounds to dismiss the BIPA claim. The court was required to determine whether Illinois or California had "a greater interest in the determination of [the] case." 185 F. Supp. 3d at 1169. In answering that question, the court found that BIPA represented a "fundamental" (i.e., substantial) "policy of the state of Illinois" and that Illinois thus had an interest in "protecting its citizens' right to privacy in their personal biometric data." *Id.* That tells us only the unremarkable proposition that the State of Illinois has an interest in protecting its citizens' privacy rights. The district court had no need to determine what BIPA's core interest was. And it did not decide whether that core interest was data protection or something as broad as what the Vigils advance here.

In *Rivera*, the court determined whether "face-scan measurements derived from a photograph … qualify as biometric identifiers." 2017 WL 748590, at *5. Even though the opinion uses the word "privacy," the court did not address what BIPA's core interest was, or whether it extended beyond data protection.

The Vigils' attempt to redefine BIPA's core interest to a more generalized privacy interest is ultimately self-defeating. The more generalized (and thus, abstract and ill-defined) the core interest of a statute supposedly is, the less concrete it becomes. As this Court emphasized in *Strubel*, a legislature's role in defining intangible harms is not unfettered. This Court must make sure that the

- 20 -

identified statutory interest is sufficiently concrete for Article III. 842 F.3d at 188-89; *see Spokeo*, 136 S. Ct. at 1549 (noting that "both history and the judgment of Congress play important roles" and that "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts").

Unfortunately for the Vigils, "loss of privacy and breach of confidentiality are too abstract to establish Article III standing." *Duqum v. Scottrade, Inc.*, 2016 WL 3683001, at *8 (E.D. Mo. July 12, 2016); *see also Bultemeyer v. CenturyLink, Inc.* 2017 WL 634516, at *4 (D. Ariz. Feb. 15, 2017) (the "post-*Spokeo* cases from around the country have uniformly found that, absent disclosure to a third party or an identifiable harm from the statutory violation, there is no privacy violation"); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015) ("[e]ven if Plaintiffs adequately allege a loss of privacy, they have failed to show how that loss amounts to a concrete and particularized injury"). Based on BIPA's included legislative findings, the district court correctly focused on BIPA's purpose of data protection to evaluate whether the Vigils have Article III standing.

C. The District Court Correctly Concluded That The Five Alleged Statutory Violations Do Not Result In Actual Harm Or Create The Material Risk Of Harm To Biometric Data Protection.

The Vigils' appeal focuses on five alleged statutory violations. *See* Appellants' Br. at 5, 29-30. Each concerns mere procedural rights designed to

protect data from breach or misuse. Even assuming that these rights were violated,

the alleged violations do not result in actual harm nor do they inherently present

any material risk of harm. Thus, none can support Article III standing.

1.   Collection Of The Vigils' Biometrics

The Vigils claim that Take-Two collected their biometric information in

violation of Section 14/15(b)(1) and (3). That section states that "No private entity

may collect, capture, purchase, receive through trade, or otherwise obtain a

person's or a customer's biometric identifier or biometric information, unless it

first … informs the subject … in writing that a biometric identifier or biometric

information is being collected or stored [and] receives a written release …."

The Vigils assume that Take-Two somehow stole, coerced, or tricked them

into surrendering biometric information. They argue that by violating Sections

14/15(b)(1) and (3), Take-Two "harmed" them by collecting that information

"without authorization." The district court recognized, however, that their

lawyers' repeated use of the phrase "without authorization" does not make it so,

especially given the complaint's actual allegations, which control.

The complaint concedes that Take-Two did ***not*** collect biometric

information "without authorization." It alleges that the Vigils were aware of and

chose to use the MyPlayer feature to create a personalized avatar. Before the

Vigils could proceed, they were notified that a "face scan" would be recorded and

captured. A.23 ¶ 28. The Vigils not only affirmatively pressed "Continue" to

proceed, they sat in front of a camera, turning their heads slowly to the left and the

right for nearly 15 minutes, as their camera scanned their faces. *See* A.23-24 ¶ 29.

Thus, what the Vigils complain about is ***not*** that their faces were scanned

without authorization, but that—despite their knowledge, consent, and active

participation in the face scan—Take-Two somehow nevertheless violated the

technical requirements of Section 14/15(b)(1) and (3). The Vigils never explain

exactly what this technical violation is. Presumably, the Vigils contend that the on

screen notification was not a sufficient "writing" and that requiring them to press

"Continue" did not constitute their assent to a sufficient "written release." The

Vigils also suggest that explicit notification of a "face scan" is not sufficient

because Take-Two did not use the magic words "biometric identifier" when

communicating with them about the "face scan."

Without getting into the merits (or lack thereof) of such a violation, this

claim does not place a substantive right at stake. There is nothing in BIPA's

legislative findings suggesting that the Illinois legislature believed that the lack of

a writing was somehow *malum in se* or *per se* injurious. Nor is there any

indication the legislature sought to elevate the "writing" requirement to the status

of a new substantive right or that there should be some special obligation to use the

"biometric identifier" term of art. Rather, the right allegedly implicated is

- 23 -

procedural in nature. It is designed, in conjunction with BIPA's other requirements, to promote the core data protection interest.

The Vigils argue that, even though they knew about the "face scan," they were "completely unaware of the true nature of the technology powering the NBA 2K15 MyPlayer feature." Appellants' Br. at 31. But their ignorance of the details of how the scanning technology worked does not mean their faces were scanned without their authorization. The Vigils chose to proceed with the face scan despite their claimed ignorance of the technological details. And nothing in the legislative findings suggests that the legislature intended to create a substantive right to know the "technical details" or to impose an affirmative obligation to explain how the technology works before biometrics can be collected. As the district court found, "[t]here is no plausible allegation that, based on the notice the plaintiffs received, the plaintiffs did not understand that their faces would be scanned, and that those face scans would be used to create personalized basketball avatars." SPA.33.

As purely procedural protections, the Vigils must show how the lack of a writing somehow poses an inherent, material risk of harm. Neither the failure to require pen-and-paper authorization (as opposed to an onscreen notification and "Continue" button) nor the use of the words "face scan" instead of "biometric identifier" poses any material risk of harm to biometric data protection. Such supposed shortcomings do not make it any more likely that the data will be

misused or compromised. The Vigils do not argue otherwise, tacitly admitting

that, unless the violation is substantive, they cannot prevail on this violation.

2. Disclosure Of The Vigils' Biometrics At Their Request

The Vigils' second alleged BIPA violation fails for the same reason.

Section 14/15(d) states that "No private entity in possession of a biometric

identifier or biometric information may disclose, redisclose, or otherwise

disseminate a person's or a customer's biometric identifier or biometric

information unless … the subject of the biometric identifier or biometric

information … consents to the disclosure or redisclosure …." Appellants make

similar arguments about "consent"—here for disclosure, as opposed to collection.

Unlike BIPA's collection provision, however, its disclosure provision does not

require that the consent even be in writing. *See* 740 Ill. Comp. Stat. 14/15(d)(1)

("the subject of the biometric identifier or biometric information … consents to the

disclosure").

The complaint concedes that biometric information—here, the personalized

avatar—was disclosed with the Vigils' consent. The Vigils were notified when

they first used the MyPlayer feature that their "face scan will be visible to you and

others you play with and may be recorded or screen captured during gameplay."

A.23 ¶ 28. They consented to the scanning when they pressed "Continue," sat for

the scan, created their avatars, and used them. A.26 ¶ 41. The Vigils allege that

- 25 -

their biometric information—i.e., the avatar based on their face scans—"was disclosed and disseminated to other players" when they entered a multiplayer game. A.27 ¶ 45. But they do not deny that they chose to enter the multiplayer game, chose to use their avatar, and knew others would see it. The Vigils do not allege that their biometric data was "disseminated in any form other than to the gamers who played in multiplayer games with the plaintiffs." SPA.13.[5]

Again, the Vigils allege at most a procedural violation. Nothing about this process fails to meet Section 14/15(d). BIPA does not contain a blanket prohibition on the disclosure of biometrics; it specifically allows disclosure with an individual's "consent." 740 Ill. Comp. Stat. 14/15(d)(1)-(2). Though the Vigils repeatedly argue that 14/15(d)(1) requires either "adequate" or "informed" consent, as noted above, the statute requires only "consent" and does not require any informational or other disclosures. *Compare id.* ("the subject of the biometric identifier or biometric information … consents to the disclosure"), *with, e.g.*, A.34 ¶ 76 ("Take-Two … disclosed [the Vigils' biometrics] without first obtaining *adequate* consent.") (emphasis added); Appellants' Br. at 29 ("Take-Two disseminated the Vigils' biometric data to others during game play without their

---

[5] At oral argument, the Vigils partially abandoned their 14/15(d) claim. *See* SPA.13 n.4 ("Counsel for the plaintiffs made clear at oral argument that the plaintiffs are not seeking to base their claims on their volitional entrance into multiplayer games, where the digital renditions of their faces on the personalized basketball avatars could be viewed by third-parties."); A.358-60.

informed consent.") (emphasis added). As the Vigils admit, they consented to the only alleged disclosure in this case. Even if they can expand what Section 14/15(d) requires, the only thing that remains of the violation, given the Vigils' actions, is some unspecified procedural failure to comply with how that consent should have been obtained, if any different than how it was.

An alleged failure to comply with Section 14/15(d)'s procedural requirements does not present a risk of material harm to biometric data protection. The fact that other players in a multiplayer video game are able to view the personalized avatars that the Vigils created and chose to show to those other persons does not create a material risk that their biometrics will be compromised.

3.   Length And Purpose Of Biometric Collection

Section 14/15(b)(2) requires that any private entity that collects biometric information "inform[] the subject … in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used." 740 Ill. Comp. Stat. 14/15(b)(2).

The Vigils admit that this is a procedural violation. Appellants' Br. at 34.[6]

Appellants claim that without written information about purpose and length, "a

consumer would be … left unaware of how long his or her biometrics will be in the

hands of others; deprived of all control over his or her biometrics …; and helpless

to prevent possible future downstream collection, disclosure, or use of his or her

biometrics …." *Id.*

Regardless of whether Take-Two informed the Vigils in writing of the

length or purpose of the biometric collection, they knew that their face scans would

be retained for at least as long as they kept their avatars. *See McCollough v.*

Smarte Carte, Inc., 2016 WL 4077108, at *3 (N.D. Ill. Aug. 1, 2016) (The plaintiff

"undoubtedly understood when she first used the system that her fingerprint data

would have to be retained until she retrieved her belongings from the locker.").

That Take-Two did not provide the Vigils with the disclosures in writing, as

required by 14/15(b)(2), does not create a material risk that the Vigils' biometrics

will be compromised. *See id.* at *4 ("Even without prior written consent to retain,

---

[6] By conceding the failure to inform the Vigils in writing of this information is
procedural, the Vigils have abandoned on appeal any argument that BIPA creates a
substantive "right to information." As the district court explained, "BIPA is not
akin to a statute where the right-to-information is a concrete interest in-of-itself."
SPA.30. "Unlike statutes where the provision of information about statutory
rights, or matters of public concern, is an end itself, the BIPA's notice and consent
provisions do not create a separate interest in the right-to-information, but instead
operate in support of the data protection goal of the statute." *Id.*; *see generally*
Nokchan v. Lyft, Inc., 2016 WL 5815287, at *6 (N.D. Cal. Oct. 5, 2016).

if [the defendant] did indeed retain the fingerprint data beyond the rental period,

this Court finds it difficult to imagine, without more, how this retention could work

a concrete harm."). The Vigils do not allege an actual (or even attempted) data

breach, misuse of their information, or that Take-Two has attempted to sell or

disclose their data without their consent. *See Khan v. Children's Nat'l Health Sys.*,

188 F. Supp. 3d 524, 533 (D. Md. 2016).

Even if there is some potential risk of compromise, the Supreme Court has

made clear that "'[a]llegations of possible future injury' are not sufficient," and

speculative allegations, "which rel[y] on a highly attenuated chain of possibilities,

do[] not satisfy the [certainly impending] requirement." *Clapper v. Amnesty Int'l*

USA,, 133 S. Ct. 1138, 1147-48 (2013). The potential harms the Vigils identify are

too speculative to constitute the "material risk" required for Article III standing.

See Braitberg v. Charter Commc'ns., Inc., 836 F.3d 925, 930 (8th Cir. 2016).

4. Biometric Retention Schedule And Destruction Guidelines

Section 14/15(a) requires that a private entity in possession of biometric

information "develop a written policy, made available to the public, establishing a

retention schedule and guidelines for permanently destroying biometric identifiers

and biometric information when the initial purpose for collecting or obtaining such

identifiers or information has been satisfied or within 3 years of the individual's

last interaction with the private entity, whichever occurs first."

The Vigils fault Take-Two for "not publicly provid[ing] a retention schedule or guidelines for permanently destroying the [Vigils' biometrics]." A.34 ¶ 75; *see also* A.26 ¶ 38; Appellants' Br. at 5, 30. The Vigils admit that this too is a procedural violation. Appellants' Br. at 34.

Failing to make publicly available a retention schedule or destruction guidelines does not pose any material risk of harm to biometric data protection. The Vigils argue that, by failing to make available any retention schedule or destruction guidelines, they were deprived of their ability to ensure that those schedules or guidelines were complied with, which thereby increased the risk that their data might be compromised. Even if true, that chain of possibilities, like the others, is too attenuated to constitute a cognizable harm. Again, any risk of future harm must be "certainly impending" to be concrete. *See Clapper*, 133 S. Ct. at 1147; *see also Khan*, 188 F. Supp. 3d at 533; *Hammond v. Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, at *6 (S.D.N.Y. June 25, 2010); *Nat'l Council of La Raza v. Gonzales*, 468 F. Supp. 2d 429, 433-35, 44 (E.D.N.Y. 2007).

The Vigils do not even allege that Take-Two has retained their biometrics beyond the time period BIPA permits. Thus Take-Two can still comply with any destruction obligations, even if it failed to inform the Vigils of those obligations in a publicly available writing. It is not possible to conclude that the Vigils sustained any real injury simply because Take-Two failed to inform them of a destruction

obligation that, in the end, Take-Two has not breached. *See* 740 Ill. Comp. Stat. 14/15(a); *Strubel*, 842 F.3d at 194 ("It would be more than curious to conclude that a consumer sustains real injury to concrete TILA interests simply from a creditor's failure to advise of a reporting obligation that, in the end, the creditor honors.").

Even if Take-Two had retained biometric information longer than BIPA permits, that does not create an ***impending*** risk of a data breach or compromise. In *Braitberg*, as here, the plaintiff alleged that the defendant had retained his personal information in violation of a privacy statute. 836 F.3d at 930. The Eighth Circuit rejected this claim as a "bare procedural violation, divorced from any concrete harm," because mere retention of private information—even if wrongful—does not create any threat of imminent harm. *Id.* Similarly, in *Sterk v. Redbox Automated Retail, LLC*, the Seventh Circuit rejected the same argument that retaining information in violation of a statute created standing, explaining that "[i]f, though not timely destroyed, [the personally identifiable information] remained secreted in the video service provider's files until it was destroyed, there would be no injury." 672 F.3d 535, 538 (7th Cir. 2012). Because retention alone does not present a material risk of harm, the Vigils cannot allege any actual or imminent injury to the security of their biometric information.

5.   Biometric Transmission And Storage

Section 14/15(e) requires a private entity in possession of biometrics to use "the reasonable standard of care" within the industry to store, transmit and protect that information and to do so "in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." The Vigils allege that Take-Two violated BIPA by transmitting and storing their biometric information "on its remote server" and by transmitting their biometrics (again, the avatar) "via the open, commercial Internet, and not a secure network such as a virtual private network." A.27 ¶ 43; *see also* A.23 ¶ 26, A.25 ¶ 37, A.28 ¶ 50, A.35 ¶ 77.

Again, the Vigils admit this violation is procedural and that, to support Article III standing, it must pose a material risk of harm. Appellants' Br. at 34. As with the other violations, the Vigils' "highly attenuated chain of possibilities" falls short of the "material risk" necessary for standing. *Clapper*, 133 S. Ct. at 1148.

Regardless of the measures Take-Two uses to "store, transmit, and protect" the data, the Vigils cannot allege that there is a material risk a third party has or will imminently obtain access to it. The Vigils do not allege that their biometrics have been stolen, or even that Take-Two's servers have been breached or are likely to be breached. *See Khan*, 188 F. Supp. 3d at 533. The Vigils' subjective belief that there is "material 'risk[ ] of harm'" to the security of their data does not make

it so. *See* Appellants' Br. at 34-35; *Clapper*, 133 S. Ct. at 1152-53 ("their

subjective fear of surveillance does not give rise to standing"). Mere "speculation"

that "some unauthorized party may access" data "does not satisfy the requirement

that [they] identify an 'actual or imminent,' 'concrete and particularized' injury."

Nat'l Council of La Raza, 468 F. Supp. 2d at 444.

Even where plaintiffs have alleged an ***actual*** data breach (as opposed to the

hypothetical one the Vigils speculate might occur in the future), courts have held

that the risk of identity theft is not "certainly impending" without allegations of the

"actual misuse of the personal data or facts indicating a clear intent to engage in

such misuse with plaintiffs' data." *Khan*, 188 F. Supp. 3d at 533; *see Hammond*,

2010 WL 2643307, at *7 (allegations of increased risk "where data have been lost

and where data have been stolen" still fail to establish standing "because their

claims are future-oriented, hypothetical, and conjectural"). Without any actual

breach here, the Vigils' allegations cannot support standing.

II.   BIPA DEMANDS MORE THAN THE "BARE STATUTORY VIOLATIONS" ALLEGED BY THE VIGILS BY LIMITING ITS RIGHT OF ACTION TO A "PERSON AGGRIEVED."

BIPA limits a right of action to "[a]ny person aggrieved." 740 Ill. Comp.

Stat. 14/20. The Supreme Court has made clear that threshold requirements, such

as "person aggrieved," must be interpreted so they are not rendered irrelevant. *See*

Doe v. Chao, 540 U.S. 614, 627 (2004) (holding that person "entitled to recovery"

language requires the court to find that a plaintiff sustain an actual injury, even if

the statute includes a liquidated damages clause). This is consistent with the

Illinois rules of statutory construction, which require that a statute be construed so

that "each word, clause, and sentence, if possible, is given a reasonable meaning

and not rendered superfluous, avoiding an interpretation which would render any

portion of the statute meaningless or void." *See Sylvester v. Indus. Comm'n*, 756

N.E.2d 822, 827 (Ill. 2001).

The Vigils cannot sue under BIPA because they have not suffered any injury

and thus are not "aggrieved" persons. SPA.47. The district court followed the

reasoning of *McCollough*, which analyzed the meaning of "person aggrieved" in

BIPA and concluded that injury is required. *Id.* After canvassing other Illinois

statutes that define the term "person aggrieved," the *McCollough* court concluded

that "by limiting the right to sue to persons aggrieved by a violation of the act, the

Illinois legislature intended to include only persons having suffered an injury from

a violation as 'aggrieved.'" *McCollough*, 2016 WL 4077108, at *4.

The Vigils ask the Court to ignore *McCollough*'s discussion of "aggrieved"

because it was decided before *Strubel*. Appellants' Br. at 37-38. That makes no

sense. *Strubel* did not address the meaning of "person aggrieved."

The Illinois legislature has used the term "person aggrieved" in other statutes

to consistently require injury. For example, the Illinois Human Rights Act defines

- 34 -

"aggrieved party" as "a person who is alleged or proved to have been injured by a civil rights violation or believes he or she will be injured by a civil rights violation." 775 Ill. Comp. Stat. 5/1-103(B) (2015). Similarly, the Illinois Soil and Water Conservation District Acts defines "aggrieved party" as "any person whose property, resources, interest or responsibility is being injured or impeded in value or utility or any other manner by the adverse effects of sediment caused by soil erosion." 70 Ill. Comp. Stat. 405/3.20 (1980). Although the legislature did not define "aggrieved" in BIPA, there is no reason to believe it intended a different or lesser meaning.

That is because, in contrast to statutes like BIPA that limit a cause of action to one who is "aggrieved," other Illinois statutes permit claims to proceed based on a statutory violation alone. For example, the Illinois' Cable and Video Customer Protection Law provides that "[a]ny customer, the Attorney General, or a local unit of government may pursue alleged violations of this Act by the cable or video provider in a court of competent jurisdiction." 220 Ill. Comp. Stat. 5/22-501 (2008). In BIPA, the legislature could have authorized "any customer" to sue, but did not.

Interpreting "aggrieved" to require more than a statutory violation is supported by the courts that have interpreted that term in other contexts:

- 35 -

- In *Williams v. Merle Pharmacy*, *Inc.*, the plaintiff sued under the Illinois Wage Payment and Collection Act ("IWPCA"), which requires an employer to provided itemized payroll information to its employees. It states that "any person aggrieved" by a violation may file suit. 2015 WL 6143897, at *3 (C.D. Ill. Oct. 19, 2015). The court concluded that this phrase permitted someone who was "denied proper compensation" (i.e., injured) to bring a lawsuit, but that the IWPCA did not provide a private right of action based solely on the alleged failure to provide the itemized payroll information. *Id.* at *5. Only those with injury could sue.

- In *Padilla v. Dish Network L.L.C.*, the plaintiff alleged that the defendant's retention of his personally identifiable information violated 47 U.S.C. § 338(i)(7), which provides a claim to "[a]ny person aggrieved by any act of a satellite carrier in violation of this section." 2013 WL 3791140, at *1-3 (N.D. Ill. July 19, 2013). The court held that a person is not "aggrieved" when their personal information is wrongfully retained unless there is actual harm from that unlawful retention. *Id.* at *5.

- In *In re Colony Hill Associates*, this Court discussed the meaning of "aggrieved person" under the Bankruptcy Code, and explained that

the term requires that one be "directly and adversely affected

pecuniarily." 111 F.3d 269, 273 (2d Cir. 1997).

There is no indication that Illinois intended to depart from this well-established

understanding of the term "person aggrieved."

The Vigils rely heavily on *Glos v. People*, 102 N.E. 763 (Ill. 1913). But

Glos never considered whether the mere violation of a statute is sufficient to render

someone "aggrieved." *Glos* dealt with whether a non-party to foreclosure

proceedings had standing to appeal. The appellee was not a party in the lower

court proceedings. Concerned that her rights had been extinguished, she appealed

and asserted that she held an interest in the land. The court found that the appellee

was not "aggrieved" because, as a non-party, the lower court's decision did not

adjudicate her rights. *Glos* is unhelpful to the Vigils because there was no

statutory right at issue and there is no question that, had appellee's property rights

been adjudicated and impaired, she would have been injured in the traditional

sense. *Glos* also never defined "aggrieved" as the mere invasion of a legal right;

rather, *Glos* speaks of "a substantial grievance; a denial of some personal or

property right," which indicates that something more is required. 102 N.E. at 766.

The Vigils' other cases are similarly unhelpful. In *Greeling v. Abendroth*,

the court held that the plaintiff was aggrieved because the defendants had

interfered with a contractual relationship and deprived the plaintiff of the benefit of

a contract. 813 N.E.2d 768, 771-75 (Ill. App. Ct. 2004). The court found a specific harm, namely, that the defendant's actions "injured" or "lessened in value" plaintiff's economic interest in a bank deposit. *Id.* at 775. In *Chicago Area Council of Boy Scouts v. City of Chicago Commission on Human Relations*, the court found that the plaintiff was "aggrieved" because it was a victim of employment discrimination. 748 N.E.2d 759, 770 (Ill. App. Ct. 2001). It recognized that discrimination is one of the special circumstances where the violation of the legal right "in itself" is injurious. *Id.* None of these cases holds that a bare statutory violation that does not otherwise cause injury is sufficient.

The Vigils also cite two BIPA cases (*Rivera* and *Norberg*) but neither even so much as mentions the word "aggrieved." *See* Appellants' Br. at 38. *Rivera* held only that BIPA applied to photographs and that the alleged violations occurred in Illinois. 2017 WL 748590, at *10. In *Norberg v. Shutterfly, Inc.*, the court held that it had personal jurisdiction over the defendant and that BIPA applied to photographs. 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

This Court should uphold the district court's determination that the Vigils are not "aggrieved" and thus cannot bring a claim under BIPA. This is true regardless of whether the Vigils have standing under Article III.

III. THE DISTRICT COURT CORRECTLY DISMISSED THE COMPLAINT WITH PREJUDICE

The Vigils argue that, because the district court held that they lacked Article III standing, it should not have reached the "person aggrieved" statutory standing issue. They cite *Carter v. HealthPort Technologies, LLC*, and argue that the district court should not have dismissed their claims with prejudice if they lack Article III standing because "without jurisdiction, the district court lacks the power to adjudicate the merits of the case." 822 F.3d 47, 54-55 (2d Cir. 2016).

Take-Two agrees that a court cannot dismiss with prejudice when it lacks the power to adjudicate. Take-Two also agrees that, *in general*, a court cannot reach a statute's application if there is no Article III standing, as the court lacks the power to reach the merits. But there are exceptions. And "statutory standing" is one of them.

In *Steel Co. v. Citizens for a Better Env't*, the Supreme Court held that courts could not address merits issues without first resolving jurisdictional objections, because a court cannot proceed to adjudicate when it lacks to power to do so—precisely the basis for this Court's *Carter* decision. 523 U.S. 83, 93-95 (1998). The Supreme Court held, however, that there is a difference between a "statutory standing" question (i.e., "whether [a statute] authorizes this plaintiff to sue") and the ultimate merits (i.e., "whether the scope of the [statute's] right of action" applies or exists under the facts). *Id.* at 92. A court has the discretion and the

- 39 -

leeway to resolve the statutory standing question despite doubts about its Article

III power. *Id.; see Ruhrgas AG v. Marathon Oil Co.*, 526 U.S. 574, 584-85 (1999)

(court is not required to consider subject matter jurisdiction over other threshold

matters); *Sinochem Int'l Co. v. Malaysia Int'l Shipping Corp.*, 549 U.S. 422, 431

(2007) ("court has leeway to choose among threshold grounds for denying

audience to a case on the merits").[7]

This Court applied the *Steel Co.* distinction in *In re Facebook, Inc. Initial*

Public Offering Derivative Litigation. 797 F.3d 148, 155 (2d Cir. 2015). The

Court affirmed a district court's discretion to decide "certain threshold bases for

dismissal without deciding whether it has subject matter jurisdiction." *Id.* It held

that the district court did not overstep its Article III limits when it dismissed an

action based on a lack of statutory standing. *Id.* at 155-56 (citing *Ortiz v.*

Fibreboard Corp., 527 U.S. 815, 831 (1999) ("statutory standing … may properly

be treated before Article III standing")). This Court affirmed the district court's

discretion to look beyond the subject matter jurisdiction concerns and dismiss the

claims because the plaintiffs were not contemporaneous stock owners. *Id.* Article

---

[7] Even though the "merits inquiry and the statutory standing inquiry often 'overlap,'" there remains a difference between answering "whether *this* plaintiff has a cause of action under the statute" and "whether *any* plaintiff has a cause of action under the statute." *Steel Co.*, 523 U.S. at 99, n.2. The inquiries can be "closely connected" and "depending upon the asserted basis for lack of statutory standing, they are sometimes identical, so that it would be exceedingly artificial to draw a distinction between the two." *Id.* Nevertheless, the Supreme Court accepted this as one of those oddities that "appear in life and the law." *Id.*

III was not violated because the district court did not dismiss the actions "based on any deficiency as to the merits of the allegations pleaded" but rather "on lack of standing to proceed" under the applicable statutes. *Id.* at 156.[8]

The other Circuits agree that courts have the leeway to dismiss on threshold statutory grounds. *See, e.g*, *Niemi v. Lasshofer*, 728 F.3d 1252, 1259-60 (10th Cir. 2013) ("As a matter of state law … the plaintiffs have failed to demonstrate statutory standing to pursue any COCCA claim …. Because both this more modest state statutory standing question and any possible 'jurisdictional' problem concerning the limits of the district court's authority to issue injunctive relief in this case amount to 'threshold grounds' for resolving this appeal short of reaching its merits, we possess 'leeway to choose among' them"); *Meyers v. Oneida Tribe of Indians of Wisc.*, 836 F.3d 818, 823 (7th Cir. 2016) ("a federal court has leeway to choose among threshold grounds for denying an audience on the merits"); *ONRC Action v. BLM*, 150 F.3d 1132, 1140 (9th Cir. 1998) (decision on statutory standing may take priority over Article III standing).

---

[8] This Court observed in *American Psychiatric Association v. Anthem Health Plans, Inc.*, 821 F.3d 352 (2d Cir. 2016), that the "statutory standing" appellation can be "misleading" and "a misnomer" because it is less concerned with whether a court has the power to adjudicate a case and more with whether a plaintiff actually has a cause of action under a statute. *Id.* at 359-60. Whatever it is called, however, both the Supreme Court and this Court have held that there is a difference between a "threshold" statutory determination (i.e., is this plaintiff someone can sue under the statute) and the ultimate "merits" question (i.e., will this plaintiff prevail under the statute). Article III does not limit a court's authority to consider "threshold" determinations of entitlement to sue under a statute.

Here the district court decided whether BIPA authorizes the Vigils to bring a suit at all, i.e., whether the Vigils are "aggrieved." This threshold question is different than, for example, whether the face scans at issue are "biometric identifiers" under the statute. Because the district court has the power to adjudicate this question, it had the power to dismiss the case with prejudice. *See, e.g., Vandor, Inc. v. Militello*, 301 F.3d 37, 38-39 (2d Cir. 2002) (dismissing with prejudice even where claim was not ripe and there was no jurisdiction).

The cases discussed above make clear that the district court could have ignored the *Spokeo* issue altogether, decided the Vigils were not "aggrieved" under the statute, and simply dismissed the case with prejudice based solely on the lack of statutory standing. The leeway courts possess also means the district court can choose to address *Spokeo* instead of statutory standing, or (as it did) address both at the same time (since they flow from the same lack of harm), or decide them in the alternative. *See, e.g., United States v. BNP Paribas S.A.*, 2015 WL 1962882, at *3 (S.D.N.Y. Apr. 30, 2015) (determining petitioner lacked standing under Terrorism Risk Insurance Act of 2002 before determining that the petitioner failed to establish Article III standing, and dismissing petition with prejudice); *Howell v. Grindr, LLC*, 2015 WL 9008801, at *7 (S.D. Cal. Dec. 15, 2015) (dismissing claim for lack of statutory standing and ignoring the constitutional standing issue).

This Court has the same leeway to decide the case on either or both grounds. Indeed, to affirm the dismissal with prejudice, the Court can ignore the Article III issue and address solely the "person aggrieved" issue instead.

IV.   CONCLUSION

In the end, the Vigils are complaining about their knowing use of a videogame feature that functioned exactly as advertised and as expected. They acknowledge there has been no injury, data breach, or misuse of data. The district court correctly concluded that the Vigils lack both Article III standing and statutory standing as "persons aggrieved" to pursue a BIPA claim. Under these circumstances, the district court properly dismissed the Second Amended Complaint with prejudice. This Court should affirm that decision.

Dated: May 16, 2017   Respectfully submitted,

                                 IRELL & MANELLA LLP

                                 /s/ Robert M. Schwartz
                                 Robert M. Schwartz (rschwartz@irell.com)
                                 Victor Jih (vjih@irell.com)
                                 Nathaniel Lipanovich (nlipanovich@irell.com)
                                 Molly Russell (mrussell@irell.com)
                                 Derek R. Flores (dflores@irell.com)
                                 IRELL & MANELLA LLP
                                 1800 Avenue of the Stars, Suite 900
                                 Los Angeles, CA 90067
                                 (310) 277-1010
                                 Attorneys for Defendant-Appellee
                                 Take-Two Interactive Software, Inc.

<u>CERTIFICATE OF COMPLIANCE</u>

This document complies with the type-volume limit of Fed. R. App.

P. 32(a)(7)(B)(i) because, excluding the parts of the document exempted by Fed.

R. App. P. 32(f), this document contains 9,681 words.

This document complies with the typeface requirements of Fed. R. App.

P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because:

this document has been prepared in a proportionally spaced typeface using

Microsoft Word in 14-point Times New Roman font.

Dated: May 16, 2017   Respectfully submitted,

                               IRELL & MANELLA LLP

                               /s/ Robert M. Schwartz
                               Robert M. Schwartz (rschwartz@irell.com)
                               Victor Jih (vjih@irell.com)
                               Nathaniel Lipanovich (nlipanovich@irell.com)
                               Molly Russell (mrussell@irell.com)
                               Derek R. Flores (dflores@irell.com)
                               IRELL & MANELLA LLP
                               1800 Avenue of the Stars, Suite 900
                               Los Angeles, CA 90067
                               (310) 277-1010
                               Attorneys for Defendant-Appellee
                               Take-Two Interactive Software, Inc.